

(43)公開日 平成14年9月27日(2002.9.27)

(51) Int.Cl.	識別記号	F I	ターミナル (参考)
G 1 1 B 20/10		G 1 1 B 20/10	H 5 C 0 5 3
20/12		20/12	5 D 0 4 4
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1 5 J 1 0 4
H 0 4 N 5/91		H 0 4 N 5/91	P

審査請求 未請求 請求項の数25 O L (全 13 頁)

(21)出願番号 特願2001-76723(P2001-76723)

(22)出願日 平成13年3月16日(2001.3.16)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 郡 照彦

東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

(74) 代理人 100090376

弁理士 山口 邦夫 (外1名)

**最終頁に続く**

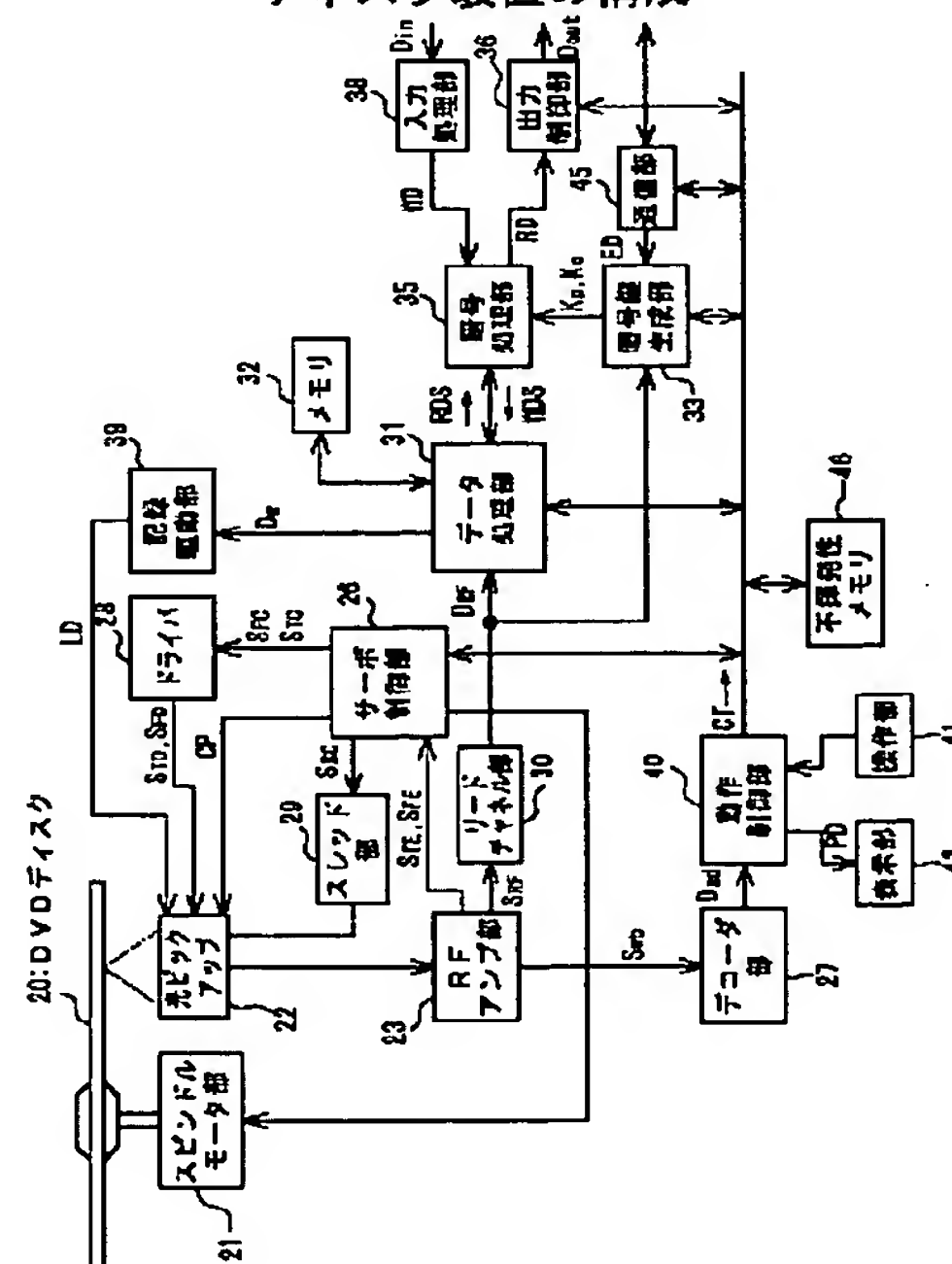
(54) 【発明の名称】 信号記録媒体とコンテンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置

(57) 【要約】

【課題】コンテンツ信号の再生の制限を容易に可能とする。

【解決手段】ディスク 20 に、再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加したコンテンツ信号を記録する。再生時に暗号鍵生成部 33 で再生制限機能を働かせることを示す制御信号が付加されていることを判別したときには、再生許可条件を満たすか否かを判別する。再生許可条件は、ディスク 20 から読み出す。また、ディスク 20 に記録されていないときには通信部 45 を介して入手する。再生許可条件を満たすときにのみ、正しい暗号鍵 Kp を暗号処理部 35 に供給する。暗号処理部 35 では、暗号化されてディスク 20 に記録されているコンテンツ信号を暗号鍵 Kp で復号化して、正しく復号化されたコンテンツ信号を出力制御部 36 から出力する。

## ディスク装置の構成



## 【特許請求の範囲】

【請求項 1】 コンテンツ信号に、該コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加し、

前記制御信号を付加したコンテンツ信号を記録したことを特徴とする信号記録媒体。

【請求項 2】 前記コンテンツ信号には、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号も付加して記録したことを特徴とする請求項 1 記載の信号記録媒体。

【請求項 3】 前記コンテンツ信号は、前記情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いて暗号化した信号であることを特徴とする請求項 1 記載の信号記録媒体。

【請求項 4】 前記コンテンツ信号は、前記情報信号と予め設定された暗号鍵と前記条件信号に基づいて生成した新たな暗号鍵を用いて暗号化した信号であることを特徴とする請求項 2 記載の信号記録媒体。

【請求項 5】 前記コンテンツ信号は、復号化が正常に完了したか否かを判別可能とする検査データを付加した信号であることを特徴とする請求項 1 記載の信号記録媒体。

【請求項 6】 コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を供給して、コンテンツ信号の再生制限動作を設定する信号生成制御手段と、前記コンテンツ信号に前記信号生成制御手段から供給された情報信号を付加して、コンテンツ流通用のコンテンツ信号を生成する信号生成手段とを有することを特徴とするコンテンツ信号生成装置。

【請求項 7】 前記信号生成制御手段では、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号の生成も行うものとし、前記信号生成手段では、前記条件信号も付加して前記コンテンツ流通用のコンテンツ信号を生成することを特徴とする請求項 6 記載のコンテンツ信号生成装置。

【請求項 8】 コンテンツ信号の暗号化を行う暗号化手段と、前記暗号化手段で前記コンテンツ信号の暗号化を行う際に用いる暗号鍵を、前記情報信号と予め設定された暗号鍵とに基づいて生成する暗号鍵生成手段とを有することを特徴とする請求項 6 記載のコンテンツ信号生成装置。

【請求項 9】 コンテンツ信号の暗号化を行う暗号化手段と、前記暗号化手段で前記コンテンツ信号の暗号化を行う際に用いる暗号鍵を、前記情報信号と予め設定された暗号鍵と前記条件信号に基づいて生成する暗号鍵生成手段とを有することを特徴とする請求項 7 記載のコンテンツ信号生成装置。

【請求項 10】 復号化が正常に完了したか否かを判別

可能とする検査データを前記コンテンツ信号に付加する付加手段を有することを特徴とする請求項 6 記載のコンテンツ信号生成装置。

【請求項 11】 コンテンツ信号を再生する際に、前記コンテンツ信号が、前記コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別するものとし、前記情報信号を有していると判別されたときには、前記コンテンツ信号の再生を許可する再生許可条件を満たしたときに、前記コンテンツ信号を出力することを特徴とするコンテンツ信号再生方法。

【請求項 12】 前記コンテンツ信号が、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号を有しているとき、前記条件信号で示された条件を満たしたときに、前記コンテンツ信号を出力することを特徴とする請求項 11 記載のコンテンツ信号再生方法。

【請求項 13】 前記コンテンツ信号が、前記再生制限機能を働かせたときに前記コンテンツ信号の再生許可条件を示す条件信号を有していないとき、前記再生許可条件の入手を行い、入手した再生許可条件を満たしたときに、前記コンテンツ信号を出力することを特徴とする請求項 11 記載のコンテンツ信号再生方法。

【請求項 14】 前記再生許可条件は、通信手段を介して、あるいは予め再生許可条件を記憶した条件記憶手段から入手することを特徴とする請求項 13 記載のコンテンツ信号再生方法。

【請求項 15】 前記再生許可条件を満たしたときには、前記制限信号と前記コンテンツ信号が有する鍵情報に基づいて暗号鍵を生成し、前記暗号鍵を用いて復号化が行われたコンテンツ信号を出力することを特徴とする請求項 11 記載のコンテンツ信号再生方法。

【請求項 16】 前記再生許可条件を満たしたときには、前記制限信号と前記コンテンツ信号が有する鍵情報と前記条件信号に基づいて暗号鍵を生成し、前記暗号鍵を用いて復号化が行われたコンテンツ信号を出力することを特徴とする請求項 12 記載のコンテンツ信号再生方法。

【請求項 17】 前記コンテンツ信号は、暗号化された信号であると共に復号化が正常に完了したか否かを判別可能とする検査データを付加した信号である場合、前記復号化を行い前記検査データによって復号化が正常に完了したと判別されたときに、前記コンテンツ信号を出力することを特徴とする請求項 11 記載のコンテンツ信号再生方法。

【請求項 18】 前記検査データによって復号化が正常に完了したと判別されないときには、コンテンツ信号の出力を行うことができないことを通知することを特徴と

する請求項 17 記載のコンテンツ信号再生方法。

【請求項 19】 コンテンツ信号が、前記コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別すると共に、前記情報信号を有していると判別されたときに、前記コンテンツ信号の再生を許可する再生許可条件を満たしている場合、前記コンテンツ信号を正しく出力可能とする設定信号の生成を行う設定信号生成手段と、

前記設定信号生成手段からの設定信号を用いて前記コンテンツ信号の出力処理を行う出力処理手段とを有することを特徴とするコンテンツ信号再生装置。

【請求項 20】 前記設定信号生成手段では、前記コンテンツ信号から前記再生許可条件を示す条件信号を抽出し、前記条件信号で示された再生許可条件を満たしたときに、前記設定信号を出力することを特徴とする請求項 19 記載のコンテンツ信号再生装置。

【請求項 21】 通信手段を有し、前記設定信号生成手段では、前記コンテンツ信号から前記条件信号を抽出できないときに、前記通信手段を介して前記条件信号を入手することを特徴とする請求項 20 記載のコンテンツ信号再生装置。

【請求項 22】 条件信号を記憶した記憶手段を予め設けるものとし、前記設定信号生成手段では、前記コンテンツ信号から前記条件信号を抽出できないときに、前記記憶手段から前記条件信号を入手することを特徴とする請求項 20 記載のコンテンツ信号再生装置。

【請求項 23】 前記設定信号生成手段では、前記条件信号で示された条件を満たしたときに、コンテンツ信号を正しく復号化する暗号鍵を設定信号として出力するものとし、前記出力処理手段では、前記コンテンツ信号の出力の際に前記暗号鍵を用いた復号化を行うことを特徴とする請求項 19 記載のコンテンツ信号再生装置。

【請求項 24】 前記コンテンツ信号に復号化が正常に完了したか否かを判別可能とする検査データが付加されている場合、前記出力処理手段では、前記復号化を行い前記検査データによって復号化が正常に完了したと判別されたときに、復号化された前記コンテンツ信号を出力することを特徴とする請求項 23 記載のコンテンツ信号再生装置。

【請求項 25】 動作状態を通知する通知手段を有し、前記出力処理手段において、前記検査データによって復号化が正常に完了したと判別されないときには、前記通知手段によってコンテンツ信号の出力を行うことができないことを通知することを特徴とする請求項 24 記載のコンテンツ信号再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、記録媒体とコン

テンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置に関する。詳しくは、コンテンツ信号に再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加するものとし、再生制限機能が働いているときには、再生許可条件を満たす場合にのみコンテンツ信号の再生を可能とすることで、コンテンツ信号の再生を制限可能とするものである。

【0002】

【従来の技術】 近年、画像・音声・テキストなどの様々なコンテンツの情報をデジタル化し統合的に取り扱うことが可能となりつつある。このように種々のコンテンツをデジタル化して配布する場合、例えば音楽や映画等が記録された記録媒体を販売する場合、記録媒体にはコンテンツがデジタル信号として記録されていることから、完全な複製を容易かつ無尽蔵に作成できてしまう。これは利用者にとっては大きな利点であるが、著作物を提供する側にとっては権利保護の面で問題となる。したがって、デジタル化されたコンテンツを配布する際には、デジタル情報としての特徴を損なわずにしかも著作権を保護できるような仕組みが実用化されている。

【0003】 この著作権保護の仕組みとして、オーディオコンテンツに対しては、例えばデジタルオーディオテープ (DAT) やミニディスク (MD) において、SCMS (Serial Copy Management System) と呼ばれるコピー制御ビットを、コンテンツ信号に設けることが行われている。このコピー制御ビットでは、コピー許可されているかコピー禁止とされているかあるいはコピーされたものであるかなどが示されており、このコピー制御ビットによって、コピー動作が制御される。またビデオコンテンツに対しては、例えば民生用デジタルビデオ規格 (DVC) や DVD-VR (Video Recording) において、CGMS (Copy Generation Management System) と呼ばれるコピー制御ビットが設けられている。このコピー制御ビットによって、コピー許可、1 世代だけコピー許可、コピー禁止あるいはコピーされたものであるかが示されており、このコピー制御ビットによって SCMS と同様にコピー動作が制御されている。さらに、DVD-AR (Audio Recording) の規格化で検討されている CQRT と呼ばれるコピー制御情報 (CCI: Copy Control Information) では、コピーを許可するか否かなどの情報だけでなく、オーディオの品質を制御する情報や関連するコンテンツ信号のコピーを許可するか否かの情報等も示されて、コピー動作をさらに詳細に制御する方法が提案されている。

【0004】

【発明が解決しようとする課題】 ところで、SCMC や CGMS 等のコピー制御は、コンテンツ信号のコピーを許可するか否かを制御するものであることから、コンテンツ信号の再生回数や再生期限等を制限することができ



ない。このため、市場に広く普及している記録媒体を利用してコンテンツの提供を行う際に、例えば再生回数や再生期限を制限してプレビューサービス等を行うものとしたり、再生回数や再生期限を制御することでコンテンツを安価に提供するなどのサービスを行うことはできない。そこで、この発明では、コンテンツ信号の再生の制限を容易に行うことができる、信号記録媒体とコンテンツ信号生成装置及びコンテンツ信号再生方法とコンテンツ信号再生装置を提供するものである。

【0005】

【課題を解決するための手段】この発明に係る信号記録媒体は、コンテンツ信号に、該コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を付加し、制御信号を付加したコンテンツ信号を記録したものである。

【0006】コンテンツ信号生成装置は、コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を供給する信号生成制御手段と、コンテンツ信号に信号生成制御手段から供給された情報信号を付加して、コンテンツ流通用のコンテンツ信号を生成する信号生成手段とを有するものである。さらに、コンテンツ信号の暗号化を行う暗号化手段と、暗号化手段でコンテンツ信号の暗号化を行う際に用いる暗号鍵を、情報信号と予め設定された暗号鍵とに基づいて生成する暗号鍵生成手段とを有するものである。また、復号化が正常に完了したか否かを判別可能とする検査データをコンテンツ信号に付加する付加手段を有するものである。

【0007】コンテンツ信号再生方法は、コンテンツ信号を再生する際に、コンテンツ信号がコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別するものとし、情報信号を有していると判別されたときには、コンテンツ信号の再生を許可する再生許可条件を満たしたときに、コンテンツ信号を出力するものである。

【0008】コンテンツ信号再生装置は、コンテンツ信号がコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かを判別すると共に、情報信号を有していると判別されたときに、コンテンツ信号の再生を許可する再生許可条件を満たしている場合、コンテンツ信号の出力を可能とする設定信号を出力する設定信号生成手段と、設定信号生成手段からの制御信号に基づきコンテンツ信号の出力処理を行う出力処理手段とを有するものである。また通信手段を有し、設定信号生成手段では、コンテンツ信号から条件信号を抽出できないときに、通信手段を介して条件信号を入手するものである。さらに、条件信号を記憶した記憶手段を予め設けるものとし、設定信号生成手段では、コンテンツ信号から条件信号を抽出できないときに、記憶手段から条件信号を入手するものである。また、動作状態を通知する通知手段を有し、出力処理手段

において、検査データによって復号化が正常に完了したと判別されないときには、通知手段によってコンテンツ信号の出力を行うことができないことを通知するものである。

【0009】この発明においては、コンテンツ信号に、このコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号が付加されると共に、この情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いてコンテンツ信号が暗号化される。

10 また、再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号も付加されると共に、この条件信号も用いて生成した新たな暗号鍵を用いてコンテンツ信号が暗号化される。この制御信号や条件信号が付加されている暗号化されたコンテンツ信号が、コンテンツ流通用の信号として記録媒体に記録されるあるいは通信回線を介して配信される。さらに、コンテンツ信号には、復号化が正常に完了したか否かを判別可能とする検査データが付加される。

20 【0010】また、コンテンツ信号の再生では、コンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号を有しているか否かが判別される。ここで、情報信号を有していると判別されたとき、コンテンツ信号が有している再生許可条件や通信回線等を介して入手した再生許可条件を満たしている場合には、情報信号と予め設定された暗号鍵とに基づいて生成した新たな暗号鍵を用いてコンテンツ信号が復号化される。また、コンテンツ信号が再生許可条件を有しているときには、この再生許可条件を示す条件信号も用いて生成した新たな暗号鍵を用いてコンテンツ信号が復号化される。

30 さらに、復号化が正常に完了したか否かを判別可能とする検査データがコンテンツ信号に付加されている場合、検査データによって復号化が正常に完了したと判別されたときに、コンテンツ信号が出力されると共に、検査データによって復号化が正常に完了したと判別されないときには、コンテンツ信号の出力を行うことができないことが通知される。

【0011】

【発明の実施の形態】以下、図を参照しながら、この発明の実施の一形態について説明する。図1は例えばDVDオーディオにおけるコンテンツの構造を示している。コンテンツは、ナビゲーション情報とメタデータ及びエレメンタリーストリームで構成される。ナビゲーション情報は、コンテンツの目次やGUI等で構成される。またメタデータは、演奏者名や歌詞などのようにコンテンツに付随した付加情報、及びコピー制御情報CCIで通常構成される。また、エレメンタリーストリームは、リニアPCMのオーディオデータやMPEG(Moving Picture Experts Group)オーディオ規格に対応したオーディオデータ等で構成される。ここで、本発明では、コンテンツ信号の再生を制限する再生制限機能を働かせるか否

かを示す制御信号である再生許可ビット(PBP: Playback Permission bit)を、メタデータに付加する。さらに、このメタデータには、再生許可条件を示す条件信号である再生条件情報(PBC: Playback Condition information)を設けることも可能とする。

【0012】図2は、コンテンツ信号の信号記録媒体であるDVD(Digital Versatile Disc)のディスク構成を示している。ディスクの最内周側にはリードイン領域が設けられており、ディスクの物理的な仕様やコンテンツ供給者の情報等が示される。このコンテンツ供給者の情報10は、後述するデータ領域に暗号化されて記録されているコンテンツを復号化するために用いるディスクキーを有している。また、リードイン領域には、BCA(Burst Cutting Area)を設けて、ディスク固有の情報、例えばディスクのシリアルIDのようなデータをレーザカッターによってバーコード状に記録することが可能とされている。リードイン領域の外周側はデータ領域とされており、このデータ領域にコンテンツ信号が記録される。データ領域の外周側にはデータ領域の終了を示すリードアウト領域が設けられており、光ビームの照射位置が、リードイン領域からリードアウト領域の範囲内で移動可能とされる。

【0013】また、DVD規格では、追記や書き換え可能なディスクである場合、UDF(Universal Disk Format)のファイルシステムが用いられる。また、再生専用のディスクの場合には、CD-ROMの規格として用いられているISO(International Organization for Standardization) 9660とUDF(Universal Disk Format)の両方の規格に対応するため、「UDF Bridge」と呼ばれるファイルシステムが用いられている。30

【0014】ここで、コンテンツ信号がオーディオのコンテンツである場合には、上述のファイルシステムにおいて、コンテンツ信号がAUDIO-TSのディレクトリ構成とされてディスクに記録される。例えば目次等がAUDIO-TS、IFOのデータ、コンテンツに付随した付加情報がATS(オーディオタイトルセット)、IFOのデータ、オーディオデータがATS、AOBのデータとされる。また、コピー制御情報CCIや再生許可ビットPBP、再生条件情報PBCは、セクタ単位で記録されたコンテンツデータのセクタヘッダ部に設ける40ものとしたり、ファイル化してデータ領域に記録する。なお、コピー制御情報CCIや再生許可ビットPBP、再生条件情報PBCの記録位置は上述の位置に限られるものではない。

【0015】ここで、AUDIO-TSのディレクトリの情報をディスクに記録して再生専用のディスクを生成する場合には、CSS(Content Scrambling System)の認証方法を用いるものとして、CPPM(Content Protection for Pre-recorded Media)と呼ばれる暗号方式でコンテンツの信号の暗号化を行い、暗号化されたコンテ50

ツ信号を用いてディスクを生成する。

【0016】図3はコンテンツ信号生成装置の構成を示す概略図である。信号生成部11では、信号生成制御部13から供給された制御信号MCSに基づいて、記憶装置12に記憶されているオーディオデータやナビゲーション情報及びコンテンツに付随した付加情報を読み出しコンテンツを構成する信号CSaを生成する。また、コピー制限や再生制限を行う場合には、信号生成制御部13からコピー制御情報CCIや再生許可ビットPBPを信号生成部11に供給して、コンテンツを構成する信号CSa内にこれらの信号を付加する。さらに、再生制限機能を動作させた場合の再生許可条件も含ませる場合には、この再生許可条件を示す再生条件情報PBCも信号生成部11に供給する。このようにして信号生成部11で生成された信号CSaは暗号処理部14に供給する。

【0017】信号生成制御部13では、上述したように信号生成部11に対して制御信号MCSや各種の情報等を供給すると共に、信号生成部11で生成された信号CSaの暗号化に用いる暗号鍵を生成するために再生許可ビットPBPや再生条件情報PBCを暗号鍵生成部15に供給する。また、信号変換部16には、リードイン領域に記録するTOC(Table Of Contents)情報TCや、信号変換動作を制御する制御信号MCFを供給する。

【0018】ここで、CPPMの暗号化を行う場合、暗号鍵生成部15では、従来のようにディスク単位の暗号鍵Keを暗号処理部14に供給するだけでなく、コンテンツ信号の再生制限機能を利用するときには、暗号鍵Keを用いるだけでなく供給された再生許可ビットPBPを用いた暗号化を行う。例えば、再生許可ビットPBPから暗号鍵Kpbpを生成して、この暗号鍵Kpbpと従来より用いられているディスク単位の暗号鍵Keとから新たな暗号鍵Kpを生成して、この暗号鍵Kpを暗号処理部14に供給する。

【0019】この新たな暗号鍵Kpの生成では、例えば再生許可ビットPBPから予め定められたアルゴリズムに基づいて暗号鍵Kpbpを生成して、この暗号鍵Kpbpと暗号鍵Keを用いて所定の演算を行い暗号鍵Kpを生成する。このとき、暗号鍵Kpの鍵長を暗号鍵Keと等しくすれば、従来の暗号化方式と鍵長の互換性を保つことができることから、再生許可ビットPBPを追加するために必要な変更点を少なくできる。また、新たな暗号鍵Kpの鍵長を暗号鍵Keよりも長くすることにより暗号強度を高めることも容易に行うことができる。また、暗号鍵Kpの生成に用いたディスク単位の暗号鍵Keを、例えばメーカー毎に割り当てられたマスター鍵Kmで暗号化して暗号鍵Ke'として信号変換部16に供給する。

【0020】また、再生条件情報PBCも用いてコンテンツ信号を生成する場合には、この再生条件情報PBCを暗号鍵生成部15に供給して再生条件情報PBCに基づく暗号鍵Kpbcを生成し、暗号鍵Ke、Kpbpだけでな



く暗号鍵K<sub>pb</sub>cも用いて新たな暗号鍵K<sub>p</sub>の生成を行う。

【0021】暗号処理部14では、暗号鍵生成部15から供給された暗号鍵K<sub>p</sub>を用いて信号C<sub>Sa</sub>の暗号化を行い信号C<sub>Sb</sub>として信号変換部16に供給する。なお、暗号鍵生成部15から、暗号処理部14に対して暗号鍵K<sub>e</sub>や暗号鍵K<sub>pb</sub>p、K<sub>pb</sub>cを別個に供給して、暗号処理部14では、それぞれの暗号鍵を用いた暗号化を繰り返し行い、このようにして得られた信号を信号変換部16に供給するものとしても良い。しかし、新たな暗号鍵K<sub>p</sub>を生成して暗号化を行うものとすれば、新たな暗号鍵の生成処理を追加するだけで、従来と同様に暗号化処理を行うことができるので、再生制限機能を設けるものとしたときの変更部分を少なくできる。なお、暗号処理部14では、信号C<sub>Sa</sub>を暗号化して信号C<sub>Sb</sub>を生成する際に、信号C<sub>Sb</sub>から再生許可ビットPBPや再生条件情報PBCを分離可能に暗号化する。

【0022】信号変換部16では、暗号化された信号C<sub>Sb</sub>と信号生成制御部13から供給されたTOC情報及び暗号鍵K<sub>e</sub>'などを用いてコンテンツ信号を生成すると共に、このコンテンツ信号を記録媒体に応じたフォーマットに変換して記録信号WAを生成する。この記録信号WAを用いてマスターディスクを生成し、このマスターディスクを用いてスタンパーを形成することで、このスタンパーを用いてコンテンツ信号の再生制限を行うことができるDVDディスクを簡単かつ容易に生成できる。

【0023】追記あるいは書き換え可能なDVDディスクでは、コンテンツ信号の記録機能を有するディスク装置によって、例えばCPRM(Content Protection for Recordable Media)と呼ばれる暗号方式で暗号化を行い、暗号化された信号をディスクに記録する。ここで、コンテンツ信号を記録する場合、ディスクには再生専用ディスクのようにディスク単位の暗号鍵K<sub>e</sub>がマスター鍵K<sub>m</sub>で暗号化されて記録されているわけではない。このため、例えば上述のリードイン領域に設けられたBCAに記録されているディスク固有の情報を利用して暗号鍵K<sub>e</sub>を生成すると共に、この暗号鍵K<sub>e</sub>を用いて暗号化を行う。あるいは、記録された楽曲を曲単位で保護出来るようにトラック毎に生成した暗号鍵K<sub>t</sub>も用いた暗号化を行う。さらに、再生制御を行うときには、上述のよう

に再生許可ビットPBPも用いて新たな暗号鍵K<sub>p</sub>を生成し、この暗号鍵K<sub>p</sub>を用いて暗号化を行う。

【0024】また、上述のCPRMの暗号化では、再生許可ビットPBPから生成した暗号鍵K<sub>pb</sub>pを用いて暗号鍵K<sub>p</sub>を生成すると共に暗号鍵K<sub>p</sub>を用いてして暗号化を行うものとしたが、再生許可条件を設定してコンテンツの再生を制限する場合には、再生許可条件を示す再生条件情報PBCをディスクに記録すると共に、この再生条件情報PBCに基づく暗号鍵K<sub>pb</sub>cを生成して、暗号鍵K<sub>e</sub>、K<sub>pb</sub>pだけでなく暗号鍵K<sub>pb</sub>cも用いて新たな暗

号鍵K<sub>p</sub>の生成を行う。

【0025】次に、上述のように再生許可ビットPBPや再生条件情報PBCも用いたコンテンツ信号の記録再生を行うディスク装置の構成を図4に示す。DVDディスク20は、スピンドルモータ部21によって所定の速度で回転される。なお、スピンドルモータ部21は、後述するサーボ制御部26からのスピンドル制御信号S<sub>sp</sub>に基づいて、DVDディスク20の回転速度が所定の速度となるように駆動される。

10 【0026】DVDディスク20には、光ピックアップ22から光量をコントロールした光ビームが照射される。DVDディスク20で反射された光ビームは、光ピックアップ22の光検出部（図示せず）に照射される。光検出部では反射された光ビームに基づき光電変換や電流電圧変換を行い、反射された光ビームの光量に応じた信号レベルの電圧信号を生成してRFアンプ部23に供給する。

20 【0027】RFアンプ部23では、光ピックアップ22からの電圧信号を用いて読出信号SRFを生成してリードチャンネル部30に供給する。また、トラッキング誤差信号STE、フォーカス誤差信号SFEを生成して、サーボ制御部26に供給する。さらに、ディスク装置が例えばDVD+RWに対応するものであるときには、ウォーブル信号S<sub>wb</sub>が生成されてデコーダ部27に供給される。

30 【0028】サーボ制御部26では、供給されたフォーカス誤差信号SFEに基づき、レーザ光の焦点位置がDVDディスク20の記録層の位置となるように光ピックアップ22の対物レンズ（図示せず）を制御するためのフォーカス制御信号SFCを生成してドライバ28に供給する。また、供給されたトラッキング誤差信号STEに基づき、光ビームの照射位置が所望のトラックの中央位置となるように光ピックアップ22の対物レンズを制御するためのトラッキング制御信号STCを生成してドライバ28に供給する。

40 【0029】ドライバ28では、フォーカス制御信号SFCに基づいてフォーカス駆動信号SFDを生成すると共に、トラッキング制御信号STCに基づいてトラッキング駆動信号STDを生成する。この生成されたフォーカス駆動信号SFD及びトラッキング駆動信号STDを光ピックアップ22のアクチュエータ（図示せず）に供給することで、光ビームが所望のトラックの中央位置で焦点を結ぶよう

50 【0030】また、サーボ制御部26では、レーザ光の照射位置がトラッキング制御範囲を越えないように、光ピックアップ22をDVDディスク20の径方向に移動させるためのスレッド制御信号SSCを生成してスレッド部29に供給する。スレッド部29では、このスレッド制御信号SSCに基づきスレッドモータを駆動して光ピックアップ22をDVDディスク20の径方向に移動させる。また、レーザ出力制御信号CPを光ピックアップ2

2に供給して、DVDディスク20に照射されるレーザー光の出力が所望のレベルとなるように制御される。

【0031】デコーダ部27では、ウォーブル信号Swbに基づきディスク上の位置を示すアドレス信号Dadを生成して動作制御部40に供給する。また、リードチャネル部30では、供給された読出信号SRFのアシンメトリ補正及び2値化を行いデジタル信号に変換して、データ信号DRFとしてデータ処理部31と暗号鍵生成部33に供給する。

【0032】データ処理部31では、データ信号DRFを8/16復調すると共にRAM(Random Access Memory)32を用いてリードソロモン積符号による誤り訂正処理等を行う。ここで誤り訂正処理がなされたデータ信号は、データ信号RDSとして暗号処理部35に供給される。

【0033】設定信号生成手段である暗号鍵生成部33では、供給されたデータ信号DRFに基づき、再生制限機能を働かせるように設定された再生許可ビットPBPを有しているか否かを判別する。ここで、再生制限機能を働かせるように設定された再生許可ビットPBPを有していると共に再生許可条件も満たしていると判別した場合には、コンテンツ信号を正しく出力可能とする設定信号、すなわち暗号化されているデータ信号RDSを正しく復号化するための暗号鍵Kpを生成して、出力処理手段を構成する暗号処理部35に供給する。また、再生制限機能が利用されていない場合や再生許可条件を満たしていないときには、従来のディスク装置と同様に暗号鍵Keを暗号処理部14に供給する。

【0034】図5は、暗号鍵生成部33の構成を示しており、暗号鍵生成部33の鍵情報抽出部331では、マスター鍵Kmで暗号化されている暗号鍵Ke'やBCA領域に記録されているディスク固有の情報を抽出して鍵生成部339に供給する。また、メタデータ抽出部332では、コンテンツのメタデータを抽出してメタデータ解析部333に供給する。

【0035】メタデータ解析部333では、抽出されたメタデータに基づいて、再生許可ビットPBPや再生条件情報PBCの検出を行う。ここで、再生許可ビットPBPが検出されて、この再生許可ビットPBPが再生制限機能を働かせるように設定されているときには、スイッチ制御信号SWCによってスイッチ334及びスイッチ335をオン状態とする。また、再生許可ビットPBPを有していないとき、あるいは再生許可ビットPBPが再生制限機能を働かせるように設定されていないときには、スイッチ334及びスイッチ335をオフ状態とする。また、再生条件情報PBCを有しているときには、スイッチ336の可動端子cを端子a側とすると共に、再生条件情報PBCを有していないときには、スイッチ336の可動端子cを端子b側に設定する。さらに、メタデータ解析部333では、再生許可ビットPBP

Pや再生条件情報PBCの検出結果を示す検出信号DTaを動作制御部40に供給する。

【0036】スイッチ334の一方の端子は再生許可ビット抽出部337と接続されると共に、他方の端子は鍵生成部339と接続されている。また、再生許可ビット抽出部337は、メタデータから再生許可ビットPBPを抽出する。この抽出された再生許可ビットPBPは、スイッチ334を介して鍵生成部339に供給される。

【0037】スイッチ335の一方の端子はスイッチ336の可動端子cと接続されると共に、他方の端子は鍵生成部339と接続されている。スイッチ336の端子aは再生条件情報抽出部338と接続されると共に、端子bは後述する通信部45と接続される。

【0038】再生条件情報抽出部338では、メタデータから再生条件情報PBCを抽出すると共に、この再生条件情報PBCで示された再生許可条件を満たすか否かを判別する。ここで、再生許可条件を満たすと判別したときには、コンテンツ信号の再生を許可する許可信号ECを生成してスイッチ336、335を介し鍵生成部339に供給する。また、再生条件情報抽出部338では、再生許可条件を満たすと判別したとき、再生条件情報PBCを鍵生成部339に供給しても良い。

【0039】また、スイッチ336に接続された通信部45を介して外部から再生許可条件を示す条件信号EDが供給されたときには、この条件信号EDをスイッチ336、335を介して鍵生成部339に供給する。

【0040】鍵生成部339では、マスター鍵Kmで暗号化されている暗号鍵Ke'を復号化して暗号鍵Keを生成する。あるいはディスク固有の情報に基づき暗号鍵Keを生成する。また、再生許可ビットPBPが再生制限機能を働かせるように設定されていると共に、許可信号ECや条件信号EDによって再生が許可されているときには、再生許可ビットPBPに基づく暗号鍵Kpbpの生成を行う。さらに、鍵生成部339では、暗号鍵Kpbpが生成されていないときには、暗号鍵Keを暗号処理部35に供給すると共に、暗号鍵Kpbpが生成されているときには、暗号鍵Keと暗号鍵Kpbpから新たな暗号鍵Kpを生成して暗号処理部35に供給する。なお、再生条件情報抽出部338から再生条件情報PBCが供給されたときには、この再生条件情報PBCに基づく暗号鍵Kpbcを生成して、この暗号鍵Kpbcと暗号鍵Keと暗号鍵Kpbpから新たな暗号鍵Kpを生成して暗号処理部35に供給する。このように、暗号鍵生成部33では、再生制限機能を利用しているか否かおよび再生許可条件を満たすか否かによって暗号処理部35に供給する暗号鍵を異なるものとする。

【0041】暗号処理部35では、暗号鍵生成部33から供給された暗号鍵を用いてデータ信号RDSの復号化を行い、得られた信号をデータ信号RDとして出力制御部36に供給する。ここで、再生許可ビットPBPを有



しており暗号鍵Kpで暗号化されたコンテンツ信号を再生する際に、暗号鍵生成部33から暗号処理部35に暗号鍵Keが供給されたときには、復号化が正しく行われていない信号がデータ信号RDとして暗号処理部35から出力制御部36に供給される。また、暗号鍵生成部33から暗号処理部35に暗号鍵Kpが供給されたときには、復号化が正しく行われた信号がデータ信号RDとして暗号処理部35から出力制御部36に供給される。なお、再生許可ビットPBPを有していないコンテンツ信号の再生では、コンテンツ信号の暗号化が暗号鍵Keを用いて行われているので、暗号処理部35から正しく復号化された信号が出力制御部36に供給されることとなる。

【0042】出力制御部36では、データ信号RDが正しく復号化が行われた信号であるか否かの判別を検査データ例えばパリティを用いて行い、正しい信号であるときには、この復号化されたデータ信号RDからパリティを除いた信号をコンテンツ出力信号Doutとして出力する。

【0043】ここで、図3の信号生成部11には、コンテンツ信号に復号化が正しく完了したか否かを判別可能とする検査データを付加する機能を持たせるものとして、オーディオデータを圧縮して記録するときには、圧縮単位例えばフレーム単位のデータ毎に検査データとして例えば上述のパリティを付加するように設定する。また、リニアPCMのオーディオデータを記録するときにも、オーディオデータを圧縮して記録する場合と同じ単位毎でパリティを付加するように設定すれば、オーディオデータがどのような信号であるかに係らず図3に示す信号生成部11や図6の出力制御部36を共用できる。

【0044】図6は、出力制御部36の構成を示している。データ信号RDは、パリティ分離部361に供給されて、コンテンツ信号に付加されているパリティPの分離が行われる。このパリティPは、上述したようにコンテンツ信号に対して所定単位毎に付加するように設定されているので、パリティ分離部361では、データ信号RDからパリティPに相当するデータを分離して比較値算出部362に供給する。また、パリティPに相当するデータが除かれたデータはスイッチ364に供給する。ここで、暗号処理部35で正しい暗号鍵を用いた復号化が行われたときには、パリティ分離部361では、正しくパリティPが分離される。また、暗号処理部35で正しくない暗号鍵を用いた復号化が行われたときには、パリティ分離部361で分離されたデータは、所定単位毎に付加したパリティPとは異なったものとなる。

【0045】比較値算出部362では、あるデータが与えられた時、このデータに対応する数値を求めることができる信号処理関数を用いて比較値RQを算出する。例えばハッシュ関数を予め設定しておくものとして、この関数にパリティ分離部361で分離されたデータを代入

することで比較値RQを算出して判定部363に供給する。

【0046】判定部363には、後述する動作制御部40から正しいパリティPを用いて求めた初期値RSが供給されており、この初期値RSと比較値算出部362から供給された比較値RQが等しいときには、スイッチ制御信号SWDによってスイッチ364をオン状態とする。

【0047】すなわち、出力制御部36では、パリティ分離部361でパリティとして分離されたデータが、コンテンツの信号に付加したパリティと等しい場合に、暗号処理部35で正しい暗号鍵を用いた復号化が行われたものと判別する。このとき、パリティが除かれた信号がコンテンツ出力信号Doutとして出力制御部36から出力される。

【0048】また、初期値RSと比較値RQが等しくないときには、暗号処理部35で正しくない暗号鍵を用いた復号化が行われたと判別して、スイッチ364をオフ状態とすることにより、正しくないコンテンツ信号が出力制御部36から出力されてしまうことを防止する。さらに、初期値RSと比較値RQが等しくないことを動作制御部40に通知して、動作制御部40によって後述する表示部42にコンテンツ信号の再生が制限されていることを表示する。なお、コンテンツ信号の再生が制限されていることは、音声等を利用して通知するものとしても良い。このように、コンテンツ信号の再生が制限されていることを通知することで、ディスク装置の異常によってコンテンツ信号の再生が行われない場合との区別を容易に判断できる。

【0049】次に、コンテンツ信号を記録する場合、コンテンツ信号Dinが供給されると、この信号Dinは入力処理部38に供給される。入力処理部38では、上述したように、コンテンツ信号Dinに対して所定単位毎に検査データであるパリティPを付加する。また、動作制御部40から再生許可ビットPBPや再生条件情報PBCが供給されたときには、これらの信号をコンテンツ信号に付加して、DVDディスク20に記録するコンテンツ信号WDとして暗号処理部35に供給する。

【0050】暗号鍵生成部33の鍵生成部339には、再生許可ビットPBPや再生条件情報PBC等が動作制御部40から供給されて、上述のCPRMの暗号方式で示したように、ディスク固有の情報を利用した暗号鍵Keとトラック単位毎の暗号鍵Ktや再生許可ビットPBP、再生条件情報PBCを用いて新たな暗号鍵Kpを生成して暗号処理部35に供給する。

【0051】暗号処理部35では、供給された暗号鍵Kpを用いてコンテンツ信号WDの暗号化を行い、コンテンツ信号WDSとしてデータ処理部31に供給する。データ処理部31では、データ信号DRFからデータ信号RDSを生成する処理とは逆の処理を行い、コンテンツ信



号WDSから記録信号Dwを生成して記録駆動部39に供給する。記録駆動部39では、記録信号Dwに基づきレーザ駆動信号LDを生成して光ピックアップ22に供給する。光ピックアップ22では、このレーザ駆動信号によってレーザ光の出力を制御することにより、コンテンツの信号をDVDディスク20に記録する。

【0052】動作制御部40には、操作部41や表示部42が接続されており、操作部41のからの操作信号PSに基づき制御信号CTを生成して各部に供給することにより、操作部41の操作に応じた動作を行わせる。また、表示部42に表示信号PDを供給して、DVDディスク20に記録されている情報の表示やディスク装置の動作状態等を表示する。また、動作制御部40では、コンテンツ信号の暗号化や復号化及び暗号鍵の生成等の動作、及び通信部45を介した再生許可条件の入手動作、初期値RSを出力制御部36に供給して正しいコンテンツ信号のみを出力させる動作等の制御を行う。

【0053】通信部45では、DVDディスク20やディスク装置が再生許可条件を有していないときに、通信回線を介して再生許可条件の入手を行う。また、通信回線を介して種々の情報の通信を行う。さらに、ディスク装置は、不揮発性メモリ46を有しており、この不揮発性メモリ46に再生許可条件やコンテンツ信号の再生に関する情報を保持することが可能とされている。

【0054】次に、再生許可ビットPBPや再生条件情報PBCを用いたコンテンツ信号の再生動作について説明する。まず、再生制限機能を働かせるように設定された再生許可ビットPBPを有していると共に、再生条件情報PBCを有していない場合の動作について説明する。この場合には、再生条件情報PBCを入手する処理を行い、再生許可条件を満たすか否かを判別し、再生許可条件を満たすと判別されたときに再生許可ビットPBPに基づく暗号鍵Kpbpを生成して、この暗号鍵Kpbpを用いて正しい暗号鍵Kpを生成する。

【0055】例えば、コンテンツ信号の再生時に、通信部45を介してコンテンツ提供者側あるいはコンテンツの配布を管理するコンテンツ管理者側に対し再生許可条件の要求を行う。コンテンツ提供者あるいはコンテンツ管理者は、コンテンツ信号再生装置と通信を行い、いずれの装置でどのようなコンテンツ信号の再生が行われるかを判別して、コンテンツ信号の使用状況を管理する。また、要求のあったディスク装置側に供給する再生許可条件として、コンテンツ信号の再生を許可する信号を条件信号EDとして供給する。この供給された条件信号EDは、スイッチ336及びスイッチ335を介して鍵生成部339に供給される。鍵生成部339では、条件信号EDによってコンテンツ信号の再生が許可されていることから、再生許可ビットPBPに基づく暗号鍵Kpbpを生成すると共に、この暗号鍵Keと暗号鍵Kpbpを用いて暗号鍵Kpを生成して暗号処理部35に供給する。こ

のため、暗号鍵Kpを用いてコンテンツの復号化を正しく行うことができる。また、コンテンツ提供者あるいはコンテンツ管理者はディスクに再生許可ビットPBPを設けておくことで、ディスク装置側でのコンテンツ信号の再生を管理することが可能となり、コンテンツ信号の再生に対して課金することができる。なお、コンテンツの使用料の徴収は電話料金に加算しても良く、また別個に請求するなど種々の方法が考えられる。

【0056】また、再生条件情報PBCを有していない場合には、再生条件情報PBCを入手する処理が行われるので、例えば通信部45を介して再生条件情報PBCを供給することにより、コンテンツ信号を流通させてからでも、再生許可条件の設定や変更を自由に行うことが可能となり、コンテンツ信号の再生制限動作の自由度を高めることができる。

【0057】さらに、暗号鍵生成部33では、コンテンツ信号に再生制限機能を働かせるように設定された再生許可ビットPBPが付加されている場合、自動的にコンテンツ信号の再生を許可するものとし、コンテンツ信号の利用状態を示す利用情報、例えばコンテンツ信号の再生回数や再生時間をコンテンツ毎に改竄できないように不揮発性メモリ46に記憶するものとしても良い。ここで、コンテンツ提供者あるいはコンテンツ管理者は、不揮発性メモリ46に記憶されている利用情報を所定期間経過毎に通信部45を介して読み出すものとするれば、上述の場合と同様にコンテンツ信号の再生に対して課金することができる。

【0058】また、使用料を先払いして、支払った使用料分だけコンテンツの再生を可能とすることもできる。例えばコンテンツ信号の再生可能回数が購入料金に応じて設定されているプリペードカードを設けると共に、このプリペードカードの情報の読み取りや更新を行うことができるカード処理部（図示せず）をディスク装置に設ける。ここで、再生制限機能を働かせるように設定された再生許可ビットPBPを有しているコンテンツ信号を再生する場合、プリペードカードを購入してカード処理部（図示せず）に装着させる。カード処理部では、コンテンツ信号の再生回数毎に、プリペードカードの使用可能残り回数情報を順次更新するものとし、使用可能回数が無くなったときには、暗号鍵生成部33において正しい暗号鍵Kpの生成を禁止することで、コンテンツ信号の再生を購入料金分だけに制限することもできる。

【0059】次に、再生制限機能を働かせるように設定された再生許可ビットPBPと再生条件情報PBCを有している場合の動作について説明する。ここで、再生条件情報抽出部338では、コンテンツ信号から再生条件情報PBCを抽出して、再生許可条件を満たすか否かを判別するものとし、再生許可条件を満たすと判別したときには許可信号ECを鍵生成部339に供給して、鍵生成部339で正しい暗号鍵Kpの生成を行う。また、再

生許可条件を満たすと判別されないときには鍵生成部 339 への許可信号 E C の供給を停止して、鍵生成部 339 によって正しい暗号鍵 Kp が生成されることを禁止する。

【0060】例えば、再生条件情報 P B C で再生回数が表示される場合、ディスク装置では、再生制限機能を働かせるように設定された再生許可ビット P B P を有したコンテンツ信号の再生回数情報を、ディスク固有の情報やディスクのタイトル固有の情報と対応付けて不揮発性メモリ 46 に保持させる。ここで、再生制限機能を働かせるように設定された再生許可ビット P B P を有するコンテンツ信号の再生が行われたとき、不揮発性メモリ 46 に保持されている再生回数が再生条件情報 P B C で示された再生回数に達していないときには、許可信号 E C を鍵生成部 339 に供給して正しい暗号鍵 Kp を暗号処理部 35 に供給させる。また、不揮発性メモリ 46 に記憶されている再生回数に「1」を加算して、再生回数情報を更新する。その後、再生回数が再生条件情報 P B C で示された回数に達したときには、鍵生成部 339 への許可信号 E C の供給を停止して、暗号処理部 35 に正しい暗号鍵 Kp が供給されることを禁止する。

【0061】このように、再生条件情報 P B C で再生回数を指定することにより、コンテンツの再生回数が指定された再生回数で制限されるので、再生回数を制限した状態でプレビューサービス等を容易に行うことができる。

【0062】また、記録可能な領域を有するディスクを用いる場合には、この領域に再生回数を示す情報を書き込むものとしても良い。この場合には、不揮発性メモリ 46 に再生回数を示す情報を記憶させておかなくとも、コンテンツの再生回数をコンテンツの再生条件情報 P B C で示された回数に制限できる。

【0063】さらに、再生条件情報 P B C は、再生回数だけでなく再生可能期間を設定するものとしても良い。例えば、再生条件情報 P B C では、使用開始から所定日数だけコンテンツ信号の再生を許可するものとすると共に、ディスク装置では、正しい暦情報及び時刻情報を入手して、この正しい暦情報及び時刻情報を用いて動作を行うものとする。

【0064】ここで、コンテンツ信号の再生が最初に行われたときには、正しい暦情報及び時刻情報を用いて、ディスク装置の不揮発性メモリ 46 やディスクの記録可能領域にコンテンツ信号の利用開始時を登録する。その後、コンテンツ信号の再生毎に、登録されている利用開始時から再生条件情報 P B C で示された期間が経過しているか否かを判別して、再生条件情報 P B C で示された期間が経過したとき鍵生成部 339 への許可信号 E C の供給を停止する。すなわち、再生条件情報 P B C で示された期間までは、正しい暗号鍵 Kp を生成して暗号処理部 35 に供給する。その後、期間が経過したときには、

正しい暗号鍵 Kp の生成を禁止して暗号処理部 35 で復号化が正しく行われることを防止することにより、コンテンツ信号の使用を所定期間内に制限することができる。

【0065】また、上述の実施の形態では、DVD ディスクに記録されているコンテンツ信号を再生する場合について説明したが、記録媒体は DVD ディスクに限られるものではなく、他の光ディスクあるいは磁気を利用した記録媒体や半導体素子を用いて構成された記録媒体であっても良い。

【0066】さらに、再生制限を行うコンテンツ信号は、記録媒体に記録されているコンテンツ信号だけでなく、無線あるいは有線の伝送路を介して配信されるコンテンツ信号であっても良い。この場合にも、コンテンツ信号にコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号や再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号を付加することで、上述の場合と同様にコンテンツ信号の再生を制限することができる。この場合のコンテンツ信号再生装置を図 7 に示す。なお、図 7 において、図 4 と対応する部分については同一符号を付し、詳細な説明は省略する。

【0067】図 7 において、通信部 45 を介して供給されたコンテンツ信号 C S は、ハード・ディスク装置や半導体メモリ等を用いて構成されたコンテンツ記憶部 50 に蓄積される。コンテンツ信号の再生時には、コンテンツ記憶部 50 から所望のコンテンツ信号 C S が読み出されて信号処理部 51 や暗号鍵生成部 33 に供給される。

【0068】信号処理部 51 では、コンテンツ信号 C S がデータ圧縮されているときに伸長処理等を行い、伸長処理後の信号 R D S を暗号処理部 35 に供給する。暗号鍵生成部 33 では、コンテンツ記憶部 50 から読み出したコンテンツ信号 C S あるいは信号処理部 51 から出力された信号 R D S が、再生許可ビット P B P や再生条件情報 P B C を有しているか否かを検出する。さらに、検出結果及び再生許可条件を満たすか否かを判別して暗号鍵の生成を行うことで、上述の場合と同様に出力制御部 36 からのコンテンツ信号の出力を制御して、配信されたコンテンツ信号 C S に対しても再生制限を行うことができる。

【0069】また、上述の実施の形態では、コピー制限機能を高めるために暗号化されたコンテンツ信号に対して再生制限を行い、暗号化されたコンテンツ信号の復号化で用いる暗号鍵の生成や正しく復号化が行われたか否かによって、正しいコンテンツ信号の出力を制限したが、コンテンツ信号は暗号化された信号に限られるものではない。例えば、暗号化されていないコンテンツ信号に対しては、再生制限機能が有効とされて再生許可条件が満たされている場合にのみ出力を行うものとするとしても、コンテンツ信号の再生を制限できる。

## 【0070】

【発明の効果】この発明によれば、コンテンツ信号に、このコンテンツ信号の再生を制限する再生制限機能を働かせるか否かを示す制御信号が付加されると共に、このコンテンツ信号の再生時には制御信号が付加されているか否かが検出される。このため、制御信号によって再生制限機能を働かせることによって、コンテンツ信号の再生を制限することができる。

【0071】また、再生制限機能を働かせたときにコンテンツ信号の再生許可条件を示す条件信号が付加されると共に、このコンテンツ信号の再生時には再生許可条件を満たすか否かが判別されて、再生条件を満たすときにコンテンツ信号の再生が行われる。このため、再生許可条件を変更することで、コンテンツ信号の再生の制限を自由に変更することができる。

【0072】また、再生制限機能を働かせたとき、コンテンツ信号に再生許可条件を示す条件信号が付加されていないときには、コンテンツ信号の再生時に、再生許可条件が入手されて、この入手された再生許可条件を満たすときにコンテンツ信号の再生が行われる。このため、再生許可条件を付加することができないようなコンテンツ信号に対してもコンテンツ信号の再生を制限できる。また、コンテンツ信号を流通させた後からでも、自由に再生許可条件を設定することができるので、様々な再生制御動作を行うことができる。さらに、コンテンツ信号の再生を制限するために制御信号を付加するだけ良いことから、コンテンツ信号の再生を制限できるように既存の信号フォーマットを容易に対応させることができる。

【0073】また、コンテンツ信号は、再生制限機能を働かせるか否かを示す制御信号と予め設定された暗号鍵、あるいは制御信号と暗号鍵と再生許可条件を示す条件信号を用いて生成された暗号鍵によって暗号化されると共に、このコンテンツ信号の再生時には、再生許可条件を満たすときに、制御信号や予め設定された暗号鍵及び条件信号を用いて暗号化に用いた暗号鍵が生成されて、この生成された暗号鍵で復号化が行われる。このため、既存の暗号化方式を用いて暗号鍵の生成方法を変更するだけで、暗号化されたコンテンツ信号に対しても簡単にコンテンツ信号の再生を制御することができる。また、制御信号や条件信号を用いて暗号鍵が生成されるので、制御信号や条件信号が改竄されたときには正しい暗

号鍵を得ることができないと共に、制御信号や条件信号をそのまま用いて復号化を行うものでもないことから、制御信号や条件信号は暗号化しなくとも良い。すなわち、暗号化する信号が増加するものでないことから、従来のコンテンツ信号の暗号化におけるフォーマットを大きく変更することなく利用できる。

【0074】さらに、コンテンツ信号の再生が制限されたときには、表示や音声によって通知されるので、コンテンツ信号の出力が行われない原因が再生装置の異常であるか再生制限が行われたことによるものか容易に判別できる。

## 【図面の簡単な説明】

【図1】コンテンツの構造を示す図である。

【図2】DVDのディスク構成の一例を示す図である。

【図3】コンテンツ信号生成装置の構成を示す図である。

【図4】ディスク装置の構成を示す図である。

【図5】暗号鍵生成部の構成を示す図である。

【図6】出力制御部の構成を示す図である。

【図7】配信されたコンテンツ信号の再生装置の構成を示す図である。

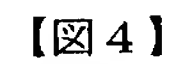
## 【符号の説明】

11・・・信号生成部、12・・・記憶装置、13・・・信号生成制御部、14・・・暗号処理部、15・・・暗号鍵生成部、16・・・信号変換部、20・・・DVDディスク、21・・・スピンドルモータ部、22・・・光ピックアップ、23・・・RFアンプ部、26・・・サーボ制御部、27・・・デコーダ部、28・・・ドライバ、29・・・スレッド部、30・・・リードチャネル部、31・・・データ処理部、33・・・暗号鍵生成部、35・・・暗号処理部、36・・・出力制御部、38・・・入力処理部、39・・・記録駆動部、40・・・動作制御部、41・・・操作部、42・・・表示部、45・・・通信部、46・・・不揮発性メモリ、50・・・コンテンツ記憶部、51・・・信号処理部、331・・・鍵情報抽出部、332・・・メタデータ抽出部、333・・・メタデータ解析部、334、335、336、364・・・スイッチ、337・・・再生許可ビット抽出部、338・・・再生条件情報抽出部、339・・・鍵生成部、361・・・パリティ分離部、362・・・比較値算出部、363・・・判定部



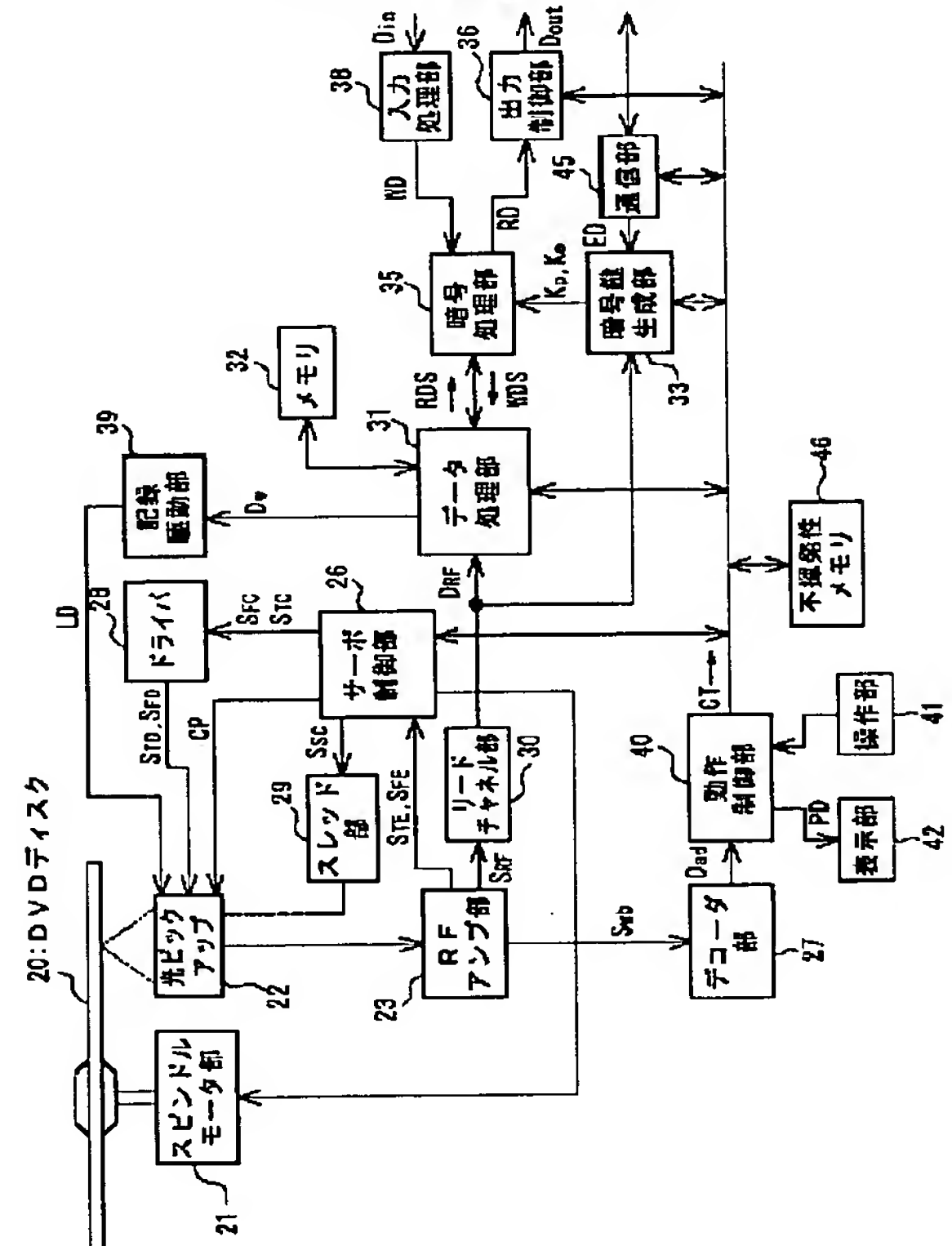
【図 2】

## DVDのディスク構成



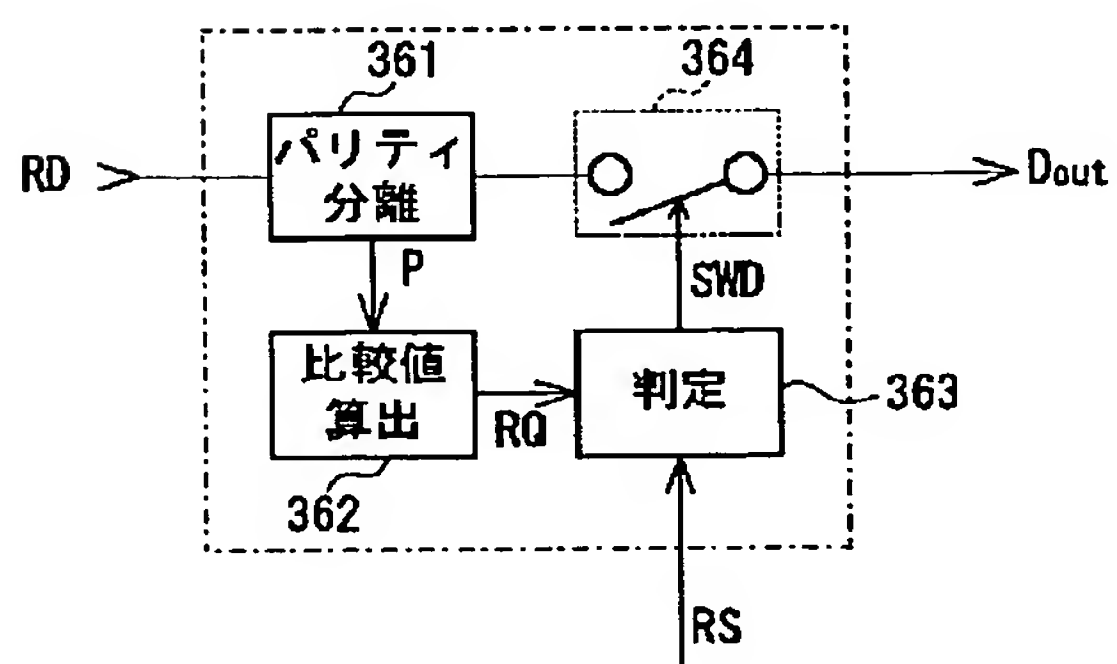
## ディスク装置の構成

## ディスク装置の構成



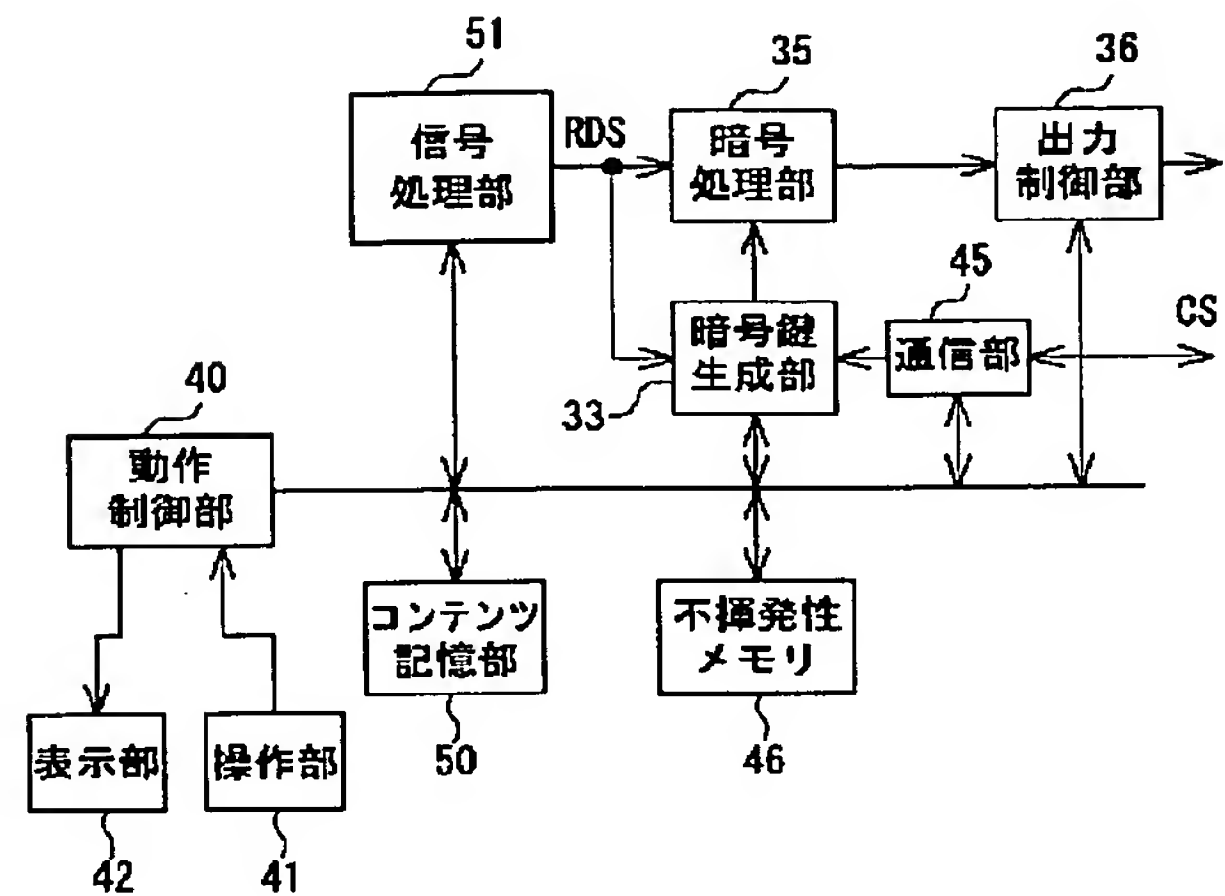
## 出力制御部の構成

## 出力制御部の構成



【図 7】

### 配信されたコンテンツ信号の再生装置の構成



Fターム(参考) 5C053 FA13 FA24 GA11 GB37 JA01  
JA21 KA01 KA08 KA16 KA24  
LA14  
5D044 AB05 AB07 BC03 CC06 DE50  
DE53 EF05 FG18 GK08 GK17  
HL08 HL11  
5J104 AA16 EA02 EA04 EA22 NA02  
PA14

This Page is inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record

## BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images  
problems checked, please do not report the  
problems to the IFW Image Problem Mailbox**